

Atty. Dkt. No. 088941-0129

IN THE CLAIMS

Claim 1. (Currently Amended) A cryptosystem key updating system for preventing illegal use of software, comprising:
encryption means for encrypting secret information;
secret information storage means for storing the secret information;
cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means;
illegal access determining means for determining whether an illegal access to the system is performed; and

cryptosystem key updating means for:

_____ providing the updated same key for a first cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a second cryptosystem key which is stored as an the updated cryptosystem key in the cryptosystem key storage means if the illegal access determining means detects no illegal access;

_____ providing different keys for the ~~above two kinds of first and second~~ cryptosystem keys if the illegal access determining means detects an illegal access; and

wherein the cryptosystem key updating means updates the ~~above two kinds of first and second~~ cryptosystem keys for each access to the system, and subsequently reencrypts the secret information stored in the secret information storage means using the updated first cryptosystem key.

Claim 2. (Currently Amended) A cryptosystem key updating method for preventing illegal use of software, the method used in a system which comprises a means for encrypting secret information; secret information storage means for storing the secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the method comprising the steps of:
determining whether an access to the system is performed;
and for each access to the system,

Atty. Dkt. No. 088941-0129

providing the same updated key for a first cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a second cryptosystem key which is stored as an the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;

providing different updated keys for the ~~above two kinds of~~ first and second cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed; and

subsequently reencrypting the secret information stored in the secret information storage means using the updated first cryptosystem key.

Claim 3. (Currently Amended) A storage medium storing a computer-executable cryptosystem key updating program for preventing illegal use of software, the program used in a system which comprises means for encrypting secret information; a secret information storage means for storing secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the program including the processes of:

determining whether an illegal access to the system is performed; and
for each access to the system,

providing the same updated key for a first cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a second cryptosystem key which is stored as an the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;

providing different updated keys for the ~~above two kinds of~~ first and second cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed; and

subsequently reencrypting the secret information stored in the secret information storage means using the updated first cryptosystem key.

Atty. Dkt. No. 088941-0129

Claim 4. (Previously Presented) A cryptosystem key updating system for preventing illegal use of software as claimed in claim 1, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

Claim 5. (Previously Presented) A cryptosystem key updating method for preventing illegal use of software as claimed in claim 2, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

Claim 6. (Previously Presented) A storage medium storing a computer-executable cryptosystem key updating program for preventing illegal use of software as claimed in claim 3, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

Claim 7. (Previously Presented) A cryptosystem key updating system for preventing illegal use of software as claimed in claim 1, wherein the system is applied to an IC card.

Claim 8. (Previously Presented) A cryptosystem key updating method for preventing illegal use of software as claimed in claim 2, wherein the system in which the method is used is applied to an IC card.

Claim 9. (Previously Amended) A storage medium storing a computer-executable cryptosystem key updating program for preventing illegal use of software as claimed in claim 3, wherein the system in which the program is used is applied to an IC card.

Claims 10-15 (Cancelled.)